

INFORMATION OPERATIONS: A JOINT PERSPECTIVE

**A MONOGRAPH
BY
Major Randall C. Lane
Armor**



**School of Advanced Military Studies
United States Army Command and General Staff
College
Fort Leavenworth, Kansas**

Second Term AY 97-98

Approved for Public Release Distribution is Unlimited

19981207 048

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE 21 May 1998		3. REPORT TYPE AND DATES COVERED Monograph
4. TITLE AND SUBTITLE INFORMATION OPERATIONS : A JOINT PERSPECTIVE ?			5. FUNDING NUMBERS	
6. AUTHOR(S) MAJOR RANDALL C. LANE				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) School of Advanced Military Studies Command and General Staff College Fort Leavenworth, Kansas 66027			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Command and General Staff College Fort Leavenworth, Kansas 66027			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES				
12a. DISTRIBUTION / AVAILABILITY STATEMENT APPROVED FOR PUBLIC RELEASE DISTRIBUTION UNLIMITED			12b. DISTRIBUTION CODE	
13. ABSTRACT (Maximum 200 words) SEE ATTACHED				
14. SUBJECT TERMS			15. NUMBER OF PAGES 54	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	20. LIMITATION OF ABSTRACT UNLIMITED	


SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

Major Randall C. Lane

Title of Monograph: *Information Operations: A Joint Perspective*


Approved by:



COL Joseph Bolick, MA, MMAS Monograph Director



COL Danny M. Davis, MA, MMAS Director, School of Advanced
Military Studies



Philip J. Brookes, Ph.D. Director, Graduate Degree
Program

Accepted this 21st Day of May 1998

Abstract

INFORMATION OPERATIONS: A Joint Perspective by MAJ Randall C. Lane, USA, 52 pages.

This monograph examines the current Department of Defense approach to the integration of information operations on the future battlefield. Technology has become one of the driving factors as the military enters into the twenty-first century. With regards to this focus, each separate military service is capitalizing on information technological advances but not with a joint focus or shared desired endstate. Information technology and systems are an integral part to the emerging field of information operations, but without the joint efforts of each service and a central controlling element the military applications of information operations will never meet their intended purpose.

This monograph first explains what information warfare and operations are along with their military applications according to each service: the Army, Navy, Marines, and Air Force. Secondly, this paper looks at what the emerging joint doctrine states concerning the definition, employment and integration of information warfare on the future battlefield. This portion of the paper examines joint doctrine concerning the integration of information operations at the operational and strategic levels with examples of how information warfare was conducted in recent deployments in Somalia, Bosnia and the Gulf War. Thirdly, the paper analyzes the potential problems determined from comparing the different service approaches to information warfare as opposed to an integrated joint approach. Lastly, this paper explores the possible military need to create either a functional command responsible for the integration of joint informational warfare or simply maintaining the current C² structure and limiting the focus to C²W for further integration of information operations training and doctrinal employment.

The recommendations proposed in this monograph are centered on developing an integrated joint approach to the training, doctrine and employment of information operations. The recommended solution to create a separate functional command responsible for the conduct and training of information operations is centered around the joint C² structure and an information-based environment designed to exploit the fluidity of future battlefields. Information and information operations will continue to be critical in future operations, but no more critical than the means to control and effectively employ them. This monograph demonstrates that the present course chosen for the development of information operations, in support of the future military, must be altered to provide an integrated and effective joint approach to the conduct of information operations.

Table of Contents

Topic	Page
I. Introduction	1
II. Information Warfare Defined	5
III. Service Perspectives on Information Warfare:	
a. United States Army	7
b. United States Navy	10
c. United States Marine Corps	14
d. United States Air Force	16
IV. Joint Perspective of Information Warfare	19
V. Comparison of Views on Information Warfare / Operations	23
VI. Joint Information Operations Alternative	32
VII. Conclusion	39
Endnotes	42
Bibliography	47

Introduction

According to Carl von Clausewitz, the ultimate aim of war is to compel our enemy to do our will.¹ Since Clausewitz' day, the desired ends of warfare have not changed but the ways and means have been altered drastically. In Alvin Toffler's book, *The Third Wave*, he expounds that we are rapidly shifting from the Industrial Age, in which warfare was based upon attrition and maneuver, to the Informational Age, in which warfare is to some extent based upon control.² Control, in this respect, can be increased or diminished depending upon one's ability to collect, process and integrate information.

In the past decade our nation and the world in general have experienced an unlimited growth in the information industry as we transition from the industrial age into an information age. This trend has been accelerated by the advances in information technology, increased focus on technology use in education and training, as well as the relatively easy access to these technologies. Information is one of the most sought after resources in the world and with control of this element of national power comes certain capabilities. Capabilities that effect every other national instrument of power: economic, diplomatic, and military.

Throughout military history, information about the enemy and about one's own forces has been paramount to the effective conduct of warfare. The control and potential dominance of information are recurring issues in both the National Security and Military Strategies. Due to the United States' desire to maintain global influence coupled with increasingly rapid technological advances, information and information technologies have become increasingly more important in both national security and the actual conduct of

military operations. Winning the competition for informational dominance is a key factor in the maintenance of national security and global military superiority.

Information warfare is still at best an evolving term and study. Each branch of military service views informational warfare with a somewhat biased eye and each service has its own working definition. Each service: Army, Navy, Air Force and Marines, is presently examining current doctrine with regard to their respective roles in information warfare. This internal service analysis is vital to the overall evolution of information warfare, but at the same time has little, if any, cohesion in a joint approach to future warfare.

The significance of studying this problem is realized by the fact that although there are numerous position papers from each service regarding information warfare, there exists no integrating doctrine between the services. Emerging joint doctrine addresses the broad term ends, ways and means of information warfare but falls short in capitalizing on the individual capabilities of each service. Each service is so individually enamored with the latest breakthroughs in technology, communications, computers and systems that a void has developed in the considerations for an integrated employment. Information warfare is not the ends but merely another means by which the military accomplishes its assigned missions.

The objectives for military information warfare range from establishing legitimacy and support in peace operations to reducing the will of adversaries while protecting friendly capabilities and our operational reach when forces are deployed.³ The Army's definitive manual concerning the future of land warfare, TRADOC PAM 525-5: Force XXI Operations, states that: "information technology is expected to make a thousandfold

advance over the next twenty years”.⁴ If this assertion is true, then as the force structure continues to dwindle due to economic and political reasons, information technology and subsequently information warfare may become increasingly important on future battlefields. Hence, it is vital that all services of the military agree upon the doctrinal training and integration of information warfare.

Purpose & Methodology

The purpose of this monograph is to determine, “what approach should the Department of Defense (DOD) take to fully incorporate information warfare on the future battlefield?” Information warfare is conducted at all levels from strategic down to and including tactical. The primary focus of this paper will remain at the operational and strategic level and discuss two potential approaches to answer the research question. One proposed approach would be to establish a functional command responsible for the integration of Joint Informational Warfare. The other alternative is to maintain the current C² structure and limit the focus to C²W for further integration of information operations training and doctrinal employment across the service components.

This paper will use the following methodology to answer the research question. First, the paper will examine what is information warfare and its military applications according to each service: the Army, Navy, Marines, and Air Force? This portion of the paper will explain the doctrinal definitions, the concept of operations and the integration plans for information warfare from each branch’s perspective with regards to warfare in the near future. Secondly, this paper will look at what the emerging joint doctrine states concerning the definition, employment and integration of information warfare on the future battlefield. This portion of the paper will examine joint doctrine concerning

information warfare and the integration of information warfare at the operational and strategic levels. This section will also provide some examples of how information warfare was conducted in recent deployments such as Somalia, Bosnia and the Gulf War.

Thirdly, the paper will analyze the potential problems determined from comparing the different service approaches to information warfare as opposed to a joint approach. This section will compare and contrast the different service issues with information warfare versus the joint perspective. Lastly, this paper will explore the possible military need to create a separate functional command responsible for the joint integration of information warfare. This section will discuss the joint integration of information operations and the military requirements necessary to plan, prepare and execute them. This section will examine the feasibility of establishing a functional command responsible for information warfare to support all military operations. This section will also examine simply limiting the scope of IO for the military to address only the C²W aspects and allow the Combatant Commanders to be the military conduits for vertical nesting with the national objectives. The conclusion will recommend potential solutions to the structure and operational aims of information warfare on battlefields in the near future. First, however, before examining the desired approach to information warfare in the future, we must fully understand the term information warfare and all of its components.

Attempting to define a concept that already has several accepted definitions seems to be, at first glance, an insignificant task. The definition for information chosen for this paper is, however, the cornerstone from which all the potential solutions to the problem will emerge. The final definition agreed upon will dramatically affect the perspective from which the remaining points in this paper are argued.

Information Warfare Defined

Before we can adequately examine what information warfare means, the definitions of both information and warfare must be discussed first. This discussion will serve to both limit the focus of this diverse subject and set the stage for the agreed upon definition for information warfare. This analysis will also demonstrate that there is even a problem with concurrence on the accepted definitions of these two individual concepts.

Information, according to the American Heritage Dictionary, is the data, instructions or content of an intended message.⁵ This definition is significantly different than what the Army and other services consider information to entail. The Army's definition of information found in FM 100-6, *Information Operations*, is "data collected from the environment and processed into a usable form."⁶ JCS Publication 1-02, *DOD Dictionary of Terminology*, defines it as the meaning that a human assigns to data by means of the known conventions used in their representation.⁷ Probably the best capstone perspective of information is provided by Professor George J. Stein, which recognizes that in fact information is merely a means to a desired endstate:

Information in itself is a key aspect of national power and more importantly, is becoming an increasingly vital national resource that supports diplomacy, economic competition, and the effective employment of military forces.⁸

Another common misconception is that war and warfare are synonymous. They are not. War is a "state of open and declared armed hostile conflict between political units such as states or nations which may be limited or general in nature."⁹ Warfare, on the other hand, is the set of all lethal and non-lethal means undertaken to subdue or compel the will of an adversary or enemy.¹⁰ The two major differences between the definitions

are that an actual declaration of war does not need to be signed in order for the military to conduct warfare and warfare, by definition, can only be limited. This is significant for two reasons: one is that it broadens the scope of operations under the concept of warfare and two because it narrows our discussion based upon a limited application in support of both political and military objectives. This limitation is essential due to the fact that IO requires an integrated approach both militarily and with government and civilian agencies.

The military focuses on operations in support of an announced military strategy that support the national aims. The apparent difference in perspective lies in the fact that the military considers information warfare to be the military application to achieve operational or strategic information dominance, while the civilian community, to include the Department of Defense (DOD), considers information warfare as an all encompassing concept of information activities designed to achieve dominance. This difference in perspective is a point of friction that could possibly lead to further confusion or lack of focus in an integrated approach to information warfare.

Given this comparison, the definitions and the concepts of both information and warfare separately, the following definition, from the Office of the Secretary of Defense, is what this paper will accept and use as the definitive meaning of information warfare for our discussion. The most comprehensive definition that focuses on the military uses states that information warfare is "actions taken to achieve information superiority in support of the National Military Strategy (NMS) by affecting the adversary information and information systems while leveraging and protecting friendly information and information systems."¹¹ Meaning that information warfare in its broadest sense is simply the military application of information and information systems to achieve desired national objectives.

Army

Focusing on the military objectives, this paper will first examine information warfare from the perspective of the United States Army. The Army actually has definitively accepted doctrine for information warfare. However, unlike the majority of the other services, the Army has doctrinal issues whether to address information operations or the more specific information warfare. According to the Army there are substantial differences between information warfare and information operations.

Information operations, according to FM 100-6, *Information Operations*, are:

Continuous military operations within the military information environment that enable, enhance, and protect the friendly force's ability to collect, process, and act on information to achieve an advantage across the full range of military operations. Information operations include interacting with the global information environment and exploiting or denying an adversary's information and decision capabilities.¹²

From this definition there appears to be very little difference between information warfare and information operations. The subtle differences are that the Army acknowledges that information operations are a larger entity covering a broader spectrum involving military and possibly political objectives. Another difference is that information operations do not necessarily have to affect the adversary's information. Information operations, from the Army's perspective, more than adequately accomplish information warfare for land combat.

The Army acknowledges the term *information warfare* as adopted by DOD, the joint community and the other services but for right now is not willing to narrow its own focus from information operations. Several Army position papers address the need for the Army

to continue to consider the impact of information operations on a full range of military missions to include support and stability operations. As of now, the Army feels that information warfare, as addressed by our early mentioned definition, does not address the full range of information operations.

Army doctrine has established three interrelated components of information operations that include: operations, relevant information and intelligence (RII) and information systems (INFOSYS).¹³ Of these three components, operations has been given the most attention because it is the military application of the entire information operation spectrum and it has a direct impact on achieving information dominance in any given environment from peace to war. Information dominance is considered to be the degree of information superiority that allows the possessor to use information systems and capabilities to achieve an operational advantage, while denying those capabilities to the adversary.¹⁴

Operations consists of Command and Control Warfare (C²W), Civilian Affairs (CA), and Public Affairs (PA). C²W is the focal point of operations given that it has the most impact in any given operational environment and the fact that it incorporates the other two components at all levels. C²W focuses on linking and protecting the information systems from national to operational level with RII support. C²W is the cornerstone of the operations component and is also the conduit to the joint and other service doctrine concerning information operations.

C²W consists of five elements including: Operational Security (OPSEC), Deception, Psychological Operations (PSYOP), Electronic Warfare (EW), and Physical Destruction and Protection.¹⁵ Given this structure inside the Army, it is clear that C²W is the action arm of both information operations and ultimately information warfare. This action arm is

intended to affect the decision-making abilities and the information support systems of any adversary.

The Army has also established an Information Operations Task Force (IOTF) designed specifically to study the applications of information operations and wargame potential functions on the future battlefield. The Army's approach is presently centered on technological advances and capabilities. The Army recognizes that control is characterized by understanding and influencing a complex structure known as the infosphere. The infosphere is a rapidly growing global network of military and commercial command, control, communications, and computer systems with networks linking information databases that are accessible to the warrior anywhere, anytime, to include during the performance of a given mission.¹⁶

One of the initiatives that the Army has exercised within the past decade is to establish a Land Information Warfare Activity at Fort Belvoir, Virginia in 1994. The creation of this center was intended to provide the Army with a service level agency to monitor, plan and execute IW and C²W for all land components involved in information operations. This activity was also initially designed to initiate connectivity with the other services, joint agencies and national level systems.¹⁷ Although this activity still exists, it appears that it is not a command and control element and has little influence in the direction of information operations for the Army of the future. More recently, the Army has been involved in more peace operations than conventional warfare and thus the prevalent focus for IO has been in the application during these operations other than war. The Army, however, still recognizes the subtle differences between IO and IW and has chosen to pursue information operations as its operational term and command and control warfare as

its limited focus for IW in both sustainment and support operations as well as conventional warfare.

Information warfare, in the form of C²W, has been integrated in the Army's tactical and operational planning for quite a while. The Army has been practicing forms of deception, psychological operations, electronic warfare and operational security for over four decades. The Army's plan to integrate IO is concentrated on the tactical and operational employment of information operations to further the military actions towards achieving operational goals.¹⁸ This means that the Army intends to integrate IO and C²W as combat multipliers to enhance combat operations in war or promote potential stability during peace operations. The Army however, still only addresses information operations in a few manuals and it is not integrated at all potential levels of application.

Due to the Army's shrinking forward presence globally, the Army sees its uses of information operations as stabilizing or enabling. With the down-sizing of the force, the force projection timeline is slower than it has ever been and there will be little chance for using IO as a deterrent element. The Army is not expecting, as part of its concept for information operations, to operate individually nor directly address national goals or objectives. The United States Navy, on the other hand, can immediately address national objectives but has very little written unclassified doctrine and has a tendency to rely on joint publications for resolution on issues and focus for levels of application.

Navy

Naval doctrine does acknowledge information warfare. The Navy, however, considers information warfare and command and control warfare almost synonymous. The majority of Naval documents concerning IW/C²W are classified and will not be discussed in this

paper. The accepted definition for information warfare from the Navy's perspective is that IW or C²W seeks to deceive, disrupt or destroy the adversary's information infrastructure and command and control process to subdue the opposition rapidly.¹⁹

The Department of the Navy, like the other services realizes the need to focus on the potential shift in emphasis for the future of warfare. The Navy recognizes that information warfare has yet unrealized capabilities that will have diverse implications in the ways that Naval forces influence, deter or, if necessary, fight and win future wars.²⁰ The Navy has long depended on information to control its own forces in a much more widely dispersed medium for conducting operations. Information and its control implications have driven the development of Naval military technology, weapon systems and information technology since the end of World War I.

Today the United States Navy operates under an initiative in command, control, communications, computers and intelligence (C4I) known as *Copernicus*. The Navy developed this C4I system in 1990 in an attempt to remain responsive to the rapidly changing technology, information systems and the impact on the warriors.²¹ Since that time, *Copernicus* has developed into the cornerstone initiative for the Department of the Navy and is responsible for shaping its training and doctrine for information warfare. In the past eight years the Navy has witnessed the prominent role of information warfare and understands the benefits to systematically using information systems to influence the outcome of future military operations.²²

Information warfare is a critical component of this C4I systems that are still under development. Likewise, information acquisition and management are some of the most important enabling factors for the Naval Expeditionary Forces during deployment.

Therefore, a large part of the operational employment is both dependent on these systems and actually developed to enhance their capabilities. Thus, given this structure it is logical to ensure that this system is capable of handling information warfare on both an operational and strategic level.

Looking more at the operational level, the Navy recognizes that the joint doctrine for C²W, *Joint Pub 3-13.1*, is focused more on the military applications of information warfare. They recognize that C²W by its definition focuses on operational security, deception measures, psychological operations, electronic warfare and even physical destruction. The Navy simply feels that it is not practicable to differentiate between the operational and the over-arching strategic goals for IW. It is most likely the nature and medium of naval warfare that prevents the Navy from separating or subordinating the two forms of warfare: IW and C²W.

In order to address the unique medium in which the Navy operates, the Navy plans to integrate their informational warfare doctrine into existing service and joint doctrine by addressing the following concerns. First, the Navy must imbed information warfare capabilities in the fleet to handle extended deployments at sea. The Fleet commanders are responsible for all actions once the ships leave the port and it is felt that they must have adequate resources, knowledge and connectivity to conduct IW/C²W for extended periods without outside assistance. Secondly, due to its forward presence and relative ease of global deployment, the Navy must have adequate systems in place to address national, as well as, operational objectives for information operations. The Navy's forward posture allows it to be in position when or before a crisis develops. Effective employment of IW could be used to possibly deter any enemies, potentially slow the tempo of the crisis or

influence the enemy's decision cycle.²³ The Navy views this as an extension of their age old mission to secure, or if necessary, interdict the Lines of Communication (LOCs).

Lastly, due to the nature of naval warfare, the information warfare systems, much like the design for the Copernicus C4I system, must be user-centered capitalizing on technological advances. Naval warfare today is seldom conducted by large concentrations of men or systems. Instead, naval warfare at the operational level is highly centralized and dependent on the employment of critical systems in time and space, as well as, achieving overall information, naval and air dominance. This is in accordance with the joint goal to achieve information superiority at all levels.

To ensure that these concerns are addressed in the Navy's emerging doctrine on information and command and control warfare, they have distributed the responsibilities by establishing three specialized organizational elements. The first is the Director of Space and Electronic Warfare (D-SEW) who is the overall responsible agency for IW/C2W development and guidance. This director works for the Deputy Chief of Naval Operations.

The second agency is the Fleet Information Warfare Center (FIWC) which is the principal agent responsible for training and procedures. And the third agency is the Naval Information Warfare Activity (NIMA) which acts as the interface between the services and the National Information Warfare organizations.²⁴ The NIMA could have potentially the most impact on the synchronized efforts of information warfare for the future. At a minimum, the NIWA can ensure that both the Navy and the Marine Corps are in unison with their approaches toward the challenge of information operations.

Marine Corps

From the Navy's perspective, the United States Marine Corps is in synch with the Navy concerning the overall goals, issues and concerns about information warfare. The Marine Corps, however, only considers information operations and not information warfare. According to the Marine Corps, information operations are actions taken to affect adversary information systems while defending one's own information and information systems.²⁵ The Marine Corps goes into more detail by explaining that IO is integrated into the concept known as *Operational Maneuver from the Sea* (OMFTS) in which the military forces use information systems and capabilities to enhance the warfighting functions of command and control, fires, intelligence, logistics and force protection.²⁶

As the Marine Corps is writing their emerging doctrine on information operations, they are approaching it from a somewhat different aspect than their parent organization: the United States Navy. The Marine Corps views information operations as an enabling factor that is "not just another arrow in the MAGTF commander's quiver, but more a broad-based capability that makes the entire bow stronger."²⁷ Taking this approach, the Marine Corps is not attempting to establish a separate organization or doctrine for information operations. Instead, information operations considerations will be added to every warfighting publication to ensure an integrated approach to addressing this new issue.

The Marine Corps structure for information operations is built along a general three pillar approach which consists of force enhancement, force protection and battlespace shaping activities. Under these three general approaches lies two distinctive elements of

information operations that integrate the more general approaches. According to the Marine Corps, information operations consists of offensive IO and defensive IO accompanied by related activities such as civil and public affairs.²⁸ The primary focus for these two elements of IO is at the operational and tactical levels. The Marine Corps acknowledges that information operations are conducted on the strategic level, however, that is a level at which the Marine Corps feels its role will be to attain some operational objective in support of some national agency.

For offensive IO, the adversary commander and his decision-making process is the ultimate target. Offensive IO involves the integration of such capabilities as computer network attack and command and control warfare (C²W). The Marine Corps' view of C²W is similar to both the Army and the Navy in that it is comprised of deception, psychological operations, operations security, electronic warfare and physical destruction. The Marine Corps acknowledges that some aspects of offensive IO are ongoing both during conflict and peacetime. In particular electronic warfare and operational security are continuous processes that require a constant quest to dominate those areas.

Defensive IO is grounded in the elements of information and information systems protection. The elements of defensive information operations are physical security, information assurance, electronic protection, counter deception, counter intelligence and counter reconnaissance. Defensive IO seeks to integrate protection, detection and reaction capabilities to deter or influence enemy actions and create an atmosphere more suitable and secure for friendly information operations.²⁹

The Marine Corps' integrated process of overlaying information operations on their existing structure is an attempt to focus their efforts on the assigned operational

objectives. The over-arching concept of *Operational Maneuver from the Sea* (OMFTS) is the guiding principle by which all other supporting initiatives are evaluated. Each supporting initiative, such as information operations, must enhance or enable the traditional elements of combat power and conducted continuously to have any merit. The Marine Corps understands that in other forms IO has been present for a long time but now it is critical to have detailed and integrated planning to be successful given the threat and the emerging capabilities of potential adversaries.

Air Force

The United States Air Force also understands the emerging threat and technological advances in information operations. The Air Force is a technology-based organization which, due to its medium of operation - similar to the Navy, deals in dispersed systems and relies heavily upon information and information systems. According to the Air Force, "information warfare is information operations conducted during a time of conflict or crisis to achieve or promote specific objectives over an adversary or adversaries."³⁰ The term information warfare has almost completely replaced the term of C²W within the Air Force doctrine.

The Air Force takes the same approach to information operations as it takes to conducting other operational campaigns. It believes in establishing superiority prior to conducting detailed operations. Information superiority, from the Air Force perspective, is the degree of dominance in the informational domain which allows the conduct of friendly information operations without effective interference.³¹ This belief is based upon a large assumption that information operations, conducted by any given adversary, can be

quantitatively measured. It is this principle, however, which is at the core of information operations for the Air Force.

In order to gain this information superiority or even dominance, the Air Force plans to concentrate its doctrine on the integration of information operations at the operational and tactical levels. Like the Marine Corps, the Air Force also believes that information operations at the strategic level will be planned by agencies outside the services who have a better handle on the national objectives. The operational objectives for information operations, however, must still support the national aims and when tasked the Air Force acknowledges that it will support the strategic applications of IO.

The Air Force's primary planning will focus on implementing IO/IW capabilities through the existing air component commands.³² Information warfare will be integrated within the normal air campaign planning model and execution process. Every aspect of air campaign planning will consider IW / C²W considerations to enhance the planning process. Information warfare will, if incorporated correctly, be a seamless operation merely requiring additional assets, considerations and training.

Given this monumental task, the Air Force has developed an Information Warfare Squadron (IWS) out of 9th Air Force to study, train and augment information operations around the world. This squadron is specialized in that its equipment is state of the art and its personnel are focused on the capabilities and vulnerabilities of information systems. This squadron augments or establishes Information Warfare (IW) teams during times of crisis to plan and execute IW integration into existing joint and space operation plans (JASOP).³³ This squadron is still in its inception and is a learning organization evolving into a viable tool for the COMAFFOR.

Once this squadron is fully on line with the Air Force operations, their integration plan calls for these squadrons to act much like a JFAAC would in a joint environment. The IW teams would be responsible for planning, developing and implementing an information campaign that supports the overall Air Component Commander's (ACC) operational plan. The IW teams would accept input from all elements of the participating air components, evaluate priorities, in line with the ACC's guidance and intent, and develop a cohesive approach to implementing an informational campaign.

The Air Force also established an Air Force Information Warfare Center (AFIWC) in September of 1993. This center is located at Kelly AFB, San Antonio, Texas. It is responsible for supporting operations, campaign planning, acquisition and testing of information systems for use in operations. The Air Force tends to classify these organizations as specialized information warfare due to their operational and tactical focus.

According to the Air Force, information warfare has six components: psychological operations, military deception, security measures, electronic warfare, information attack, and physical destruction. These components are not that different than what has been discussed earlier. The Air Force has chosen to incorporate offensive and defensive tasks in attempt to create more encompassing elements of information warfare for integration into air operations. The component that is significantly different in its approach is the direct information attack component targeting the adversary.

Information attack is involved in directly disrupting information without visible damage or change to the actual structure or entity upon inspection.³⁴ Direct information warfare, which is the more general aspect of information attack, is designed to act on the adversary's OODA loop by creating misconceptions, false observations, skewing

orientation or actually decapitating the decision-maker by imposing decisions and causing irrelevant actions.³⁵ This incapacitation of the adversary leader's abilities is one of the overall operational objectives of information attack and subsequently information warfare.

The other aspects from which the Air Force feels it can contribute to the operational realm of information operations are to deter aggression, counter WMD, support counter-terrorism and, due to the Air Force's rapid deployability, promptly influence both friendly and adversary behavior in accordance with desired theater and indirectly national objectives.³⁶ The Air Force actually views information as a fifth medium in addition to air, space, sea and land. Because there are few distinct boundaries in this given medium and the similarities that can be drawn with the air medium, the Air Force feels that they are the perfect service to lead an integrated approach to information operations. However, integrated can only truly be integrated if all services agree upon the training, doctrine and focused employment of information operations or warfare .

Joint Perspective of Information Warfare

Even though each separate service is in the process of developing their own doctrine on information warfare, there is still no agreed upon binding document to merge the collective ideas together. From the joint perspective, there is "no official information warfare doctrine and the efforts of the various services to describe command and control warfare as the military application of information warfare remain incomplete."³⁷ A more precise statement might be that there are a limited number of doctrinal documents that contain a comprehensive approach to IW but they are classified. However, at the unclassified level the *JCS Pub 1-02* states that information warfare is characterized by:

actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while leveraging and defending one's own information, information-based processes, information systems, and computer-based networks.³⁸

Even this definition is not exactly a "definition". It is simply the agreed upon characteristics of information warfare with an optimistic purpose of achieving information superiority. This definition does, however, establish some desired objectives in that IW is both offensive and defensive working toward information superiority from a joint perspective. The Department of Defense (DOD) dictionary of terms, the 1997 version, does not even acknowledge the term "information operations." Information Operations, however, is a concept discussed in *Joint Vision 2010* and carries a distinctly different connotation than information warfare. Information warfare, according to *Joint Vision 2010*, is a subset of IO.³⁹

According to *Joint Vision 2010*, the guiding concept document for joint doctrine into the 21st century, information operations are peacetime operations conducted to achieve informational superiority and if needed to deter adversary aggressions.⁴⁰ Information warfare, on the other hand, is information operations conducted in time of crisis or conflict intending to accomplish or advance specific objectives over one or more adversaries.⁴¹ This implies that in future joint doctrine publications information operations and warfare will be addressed as distinctly separate functions.

Another explanation for the stated differences may be that from a joint perspective, information operations is intended to address the pre-hostilities and post conflict phases of any given campaign, while information warfare will encompass the build-up, combat

operations and conflict termination phases. Both functions, however, from the joint level, must concentrate on attaining national-strategic and theater-strategic objectives by integrating a wide variety of agencies from the government, private sector and military.

Although there are several joint level references to components of information warfare, the capstone manual for providing the emerging conceptual approach to joint doctrine on information warfare continues to be *DOD Directive S-3600.1, Information Warfare*.⁴² This document is the unclassified revision of the first Department of Defense directive on information warfare published in 1992. These directive, as well as the guidance for the Joint Chiefs of Staff today, was derived from the National Military Strategy in support of our national aims.

Although the Joint Chiefs of Staff have produced focused joint doctrine on several sub-elements of information warfare such as command and control warfare (*JP 3-13.1*), electronic warfare (*JP 3-51*), psychological operations (*JP 3-53*) and even information management and security (*JP 3-54*), the JCS's charter remains to produce doctrine that will provide connectivity between the National Security Strategy and the National Military Strategy.⁴³ This desired document is presently under development and is titled *Information Warfare, Joint Publication 3-13*. Atlantic Command (ACOM) has the lead in producing this doctrinal manual and is presently reviewing all other services' doctrine, as well as, conceptual works and the overall joint vision for 2010 and beyond concerning information operations and warfare. Their somewhat backward approach has been one of "reverse engineering" from the bottom, service perspective, up to the joint level to ensure a unity of effort.⁴⁴

The desired endstate for the employment of information warfare, from the joint perspective, is to ensure an information battlespace advantage and operate from a position of information superiority.⁴⁵ In order to accomplish this, the office of the Joint Chiefs of Staff has developed a strategy that focuses on actions, organizations and technology and resources involved in accomplishing information operations.⁴⁶ These three areas are oriented on operations conducted in an offensive, a defensive and an other than war scenario. This conceptual structure is the base from which both the Department of Defense and JCS can orchestrate the joint conduct of information operations. This model is graphically displayed in Figure 1 below which is extracted from the *Joint Vision 2010* document.

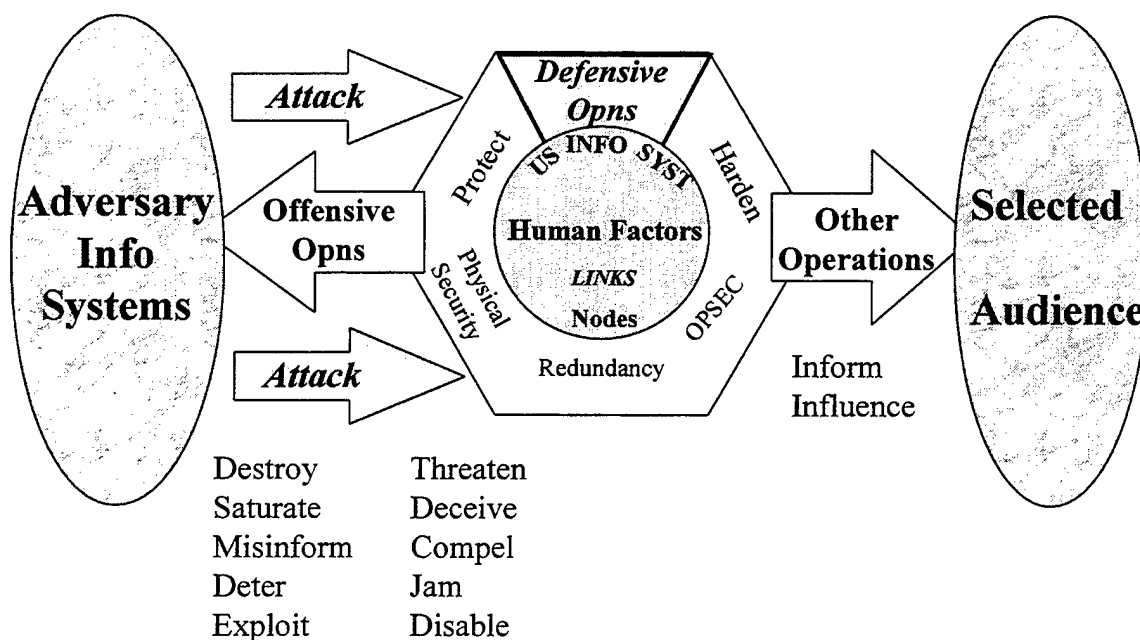


Figure 1 - Joint Information Operations Model. ⁴⁷

The clearly defined endstate of information superiority is the driving force which focuses the actions, organization and the development of technology to accomplish it. Joint doctrine, as outlined in the existing publications already mentioned and *JP 3-13*,

Information Warfare, under development, to date focus the force on the military applications of information and information systems. The emerging doctrine will attempt to integrate the existing military aspects of IW to an over-arching strategic campaign to ensure information dominance.⁴⁸ C²W will continue to be seen as the military application of information warfare but must also address operations other than war and events supporting war termination.

As the proponent for joint informational doctrine, Atlantic Command, has not yet determined whether an integrated service approach or the creation of a separate information center will meet the existing needs of the force.⁴⁹ One aspect that is certain from a joint perspective is that the management and employment of information on future battlefield's must be a coordinated and directed effort. In order to achieve an integrated approach to the operational and strategic engagement in information operations, each service must have a common understanding of the problem and an integrated concept of operation for the solutions. This is unfortunately not the case.

Comparison of Views on Information Warfare / Operations

Each service has generally the same views on the importance and future relevance of information operations or warfare. There are, however, several important differences between the services that must be examined and understood before an integrated approach can be realized. As this comparison will demonstrate, the Army and the Marines follow similar views while the Navy and the Air Force as more generally in concurrence. Both the similarities and differences can be considered from a joint perspective by analyzing the definitions, the operational concepts and finally the integration plans for future operations.

First, in order to lay the foundation for comparison, the operational definitions from each service must be compared to fully appreciate the vantage point of each individual service. The different service definitions for both information warfare and information operations are very similar, however, there are subtle differences that change the focus for the entire planning process. For example, the Army and the Marine Corps work almost exclusively with the term information operations, while the Navy and Air Force recognize both IO and IW, but are focused on the military application of information warfare. Joint doctrine excludes information operations from its existing dictionary and concentrates on information warfare. This, however, is about to change with the new doctrinal manual *JP 3-13, Information Warfare*.

The significance of this subtle difference is that the Army and Marines are focused on planning and executing information operations in both peacetime and crisis. The Navy and Air Force see their involvement in information warfare as mainly a crisis response action. These roles, however, are somewhat contradictory because the Navy and Air Force recognize that they alone possess the rapid response information capability to possibly deter before a crisis fully develops. Joint doctrine talks of the goal to achieve information superiority first in a crisis situation but, at present, does not address the ongoing struggle for informational superiority through peacetime operations. Both the Army and the Marines recognize the need for this ongoing operation because they possess minimal deterrent capabilities and must focus on stabilizing operations.⁵⁰

The perceived capabilities and desired endstate, as seen by each service, directly impact on the second point of comparison: the concept of information operations. The apparent common ground for all services is that they all focus on C²W as the focal point

for the military application of information operations or warfare. This is probably due to the fact that the *Joint Publication 3-13.1* on C²W was one of the first existing documents to demonstrate a cohesive plan for information warfare. All services are generally in concurrence with the minor exception that the Air Force, unlike the other services, considers informational attack as a means of conducting C²W. Informational attack appears to be an attempt to conduct a combination of deception, electronic warfare and physical attack from a clandestine or stealth mode of operations.

Both the Marines and Army concentrate on the military applications of IW, command and control warfare, at mainly the operational and tactical levels. The intent is to have information act as a combat multiplier to enhance either combat or peace operations. Both services acknowledge the offensive and defensive capabilities of information operations and realize that IO must be conducted in conjunction with other combat operations. Information operations, from their perspective, is not a stand alone operation capable of concluding any crisis.

Because of the focus from the Army and Marine perspective, as mentioned above, these services do not expect for information operations to operate individually or even, on most occasions, to directly address national objectives.⁵¹ By the nature of the mediums in which the soldiers from the army and marines operate, these services view IO as a continuous operation focusing on the human element. The target for IO is still the same, the human mind, but the approach is drastically different. With the proximity of forces, the Army and Marines must consider the subtleties of IO and not only focus on the larger objectives. A good example of this was seen in Bosnia. In an environment where a great

deal of information was gathered from human sources (HUMINT), the concept to drive the employment of IO was planned and executed with greater detail.

The Navy and Air Force, due to their operating media and ability to protect internal systems, are not often required to execute information warfare at such a low level. This lack of detail allows for greater speed in execution and a possible scenario where deterrence becomes an option. The rapid deployment of both the Navy and the Air Force in support of Desert Shield / Desert Storm was a good example of IW conducted to deter further aggressive actions and set the stage for later combat operations. The informational campaign initiated with these deployments exercised the first conscious national and military application of C²W with connectivity to the Global Informational network.

Each service established its own informational structure in support of this first conflict to incorporate information operations. The CINC, however, directed or refocused the objectives, priorities and concept for employment to ultimately address the national aims.⁵² CENTCOM's development of an informational warfare campaign plan was instrumental in the overall success of the operation and as such has become the cornerstone for joint doctrine development for information warfare. This adjustment at joint level was conducted late in the development process in theater and was a considerable point of conflict initially between the services due to a difference in priorities.

This concept used in Desert Storm has merit in a conventional warfare scenario, however, the concept of employment is not as clear in a support and sustain environment. Due to its extensive participation in peace operations, the Army is predominantly focused, at present, on the applications of IO in this type of environment. The Marine Corps is

likewise interested in developing doctrine to address information operations in an operations other than war (OOTW) environment, but at present has no doctrinal or position papers on the subject.⁵³ The Air Force and Navy have no existing doctrine on the application of information warfare in support and sustainment operations. Joint doctrine has an over-arching concept to integrate command and control warfare in an OOTW environment, but at present it is uncertain how this will relate to overall information warfare.

The limited focus on information operations in an OOTW environment is a serious shortcoming in the doctrinal concept of operations for either IO or IW. The implications are likewise manifested in the effects of information operations in conventional war during such stages as pre-hostilities and conflict termination. The Army and the Marine Corps are farther along with this concept due to their tactical deployments in support of such missions. The Marine Corps is approaching this issue more from a land-based perspective due to the fact that they feel this is the environment that it will mostly likely be employed.⁵⁴ Joint doctrine must address the operational and strategic linkage to fully integrate the ground, air and sea forces in support of OOTW missions.

The reason for this low level concentration by the Marines and Army can be clearly seen by looking at an example from Somalia. Mohammed Aideed, at times, succeeded in winning the information war with the U.S. through use of existing technology and small unit tactics.⁵⁵ He used cellular phones to bounce signals off walls to escape pinpointing his signals. He set up an ambush and was careful to ensure CNN was ready to cover this event. He had established a clear objective for his use of information operations and the U.S. military was unprepared to handle its effects. This is merely one example of what a

poorer country with clear objectives and the willingness to purchase and learn from technology can do to a much more powerful nation that is unprepared.

This situation described from Somalia raises another point of contention concerning the desired concept of operation for information operations. The main differences between the services' concept stems from an accepted belief in ability to attain informational dominance or superiority. The Navy, Air Force and Joint perspective is that the information warfare strategy can be simplified down to a struggle to achieve this information dominance. One potential problem with this concept is that information dominance or even superiority is something almost impossible to measure. Effects can be measured, but as was evident from the Somalia and Bosnia, effects can be deceiving. This has the potential to become a major obstacle due to the fact that the Air Force, and to an extent the Navy, considers achieving informational superiority as the first and most crucial step to any information warfare scenario.⁵⁶

The Army and Marines do not consider this objective to be attainable in all possible scenarios and merely seek to achieve a decisive advantage. Due to the fact that information technology is available to any nation with the money, this objective is becoming increasingly more difficult. Many foreign nations are presently training personnel at civilian agencies throughout the United States and will therefore soon possess the capabilities to employ these technologies. The main difference again rises from the mediums of operation. The Navy and Air Force have no real threat peer competitors. A threat peer competitor to the Army or Marine Corps is any nation capable of killing a couple of Americans and correctly timing this event to raise international or even U.S. popular support against our cause.

Information superiority is even questionable given the availability of information technology. The Navy and the Air Force are interested in shaping, or if possible deterring any given crisis, to enable future operations to be conducted in an environment more conducive to security and assured victory. The Army and the Marines are more pessimistic in their approach in that they do not believe that the military will enter any crisis from an indisputable position of superiority. These considerations in formulating a cohesive concept of operation then drive exactly how the different services approach the final point of comparison: planned integration of information operations into their existing structure.

The initial point to examine is exactly how each service views information operations or warfare. The Army and the Marine Corps view information operations as an extension of military operations or simply another combat multiplier. The Air Force views information as a fifth medium after, air, land, sea and space to be considered separately.⁵⁷ The Navy views information warfare as a separate operation in support of maritime superiority.⁵⁸ Joint doctrine calls for information warfare to be an integral part of all joint military operations.⁵⁹

Because of these views and concept for the integration of information warfare into existing military operations, each service has chosen to establish organizations to either control or facilitate the planning, preparation and execution of IO or IW. Initially the Army had established the Land Information Warfare Activity (LIWA) at Fort Belvoir, Virginia to monitor, plan and if necessary execute C²W or information operations. This organization did not prove to be an effective C² structure for information operations. It becomes very difficult to fully integrate IO when the controlling headquarters is not

within the Department of the Army chain of command and has no command authority over the combatant commands.

The Marine Corps learned from the Army's mistakes and chose to integrate information operations into existing doctrine and allow each subordinate command to incorporate IO into its planning and execution process in support of the over-arching concept of Operational Maneuver from the Sea (OMFTS). This integration plan allows the combatant commanders to evaluate the situation and fully incorporate both the naval and land capabilities at their disposal into their information campaign. The expertise is limited with this particular approach, however, it does allow more operational flexibility. The Marine Corps is concentrating on incorporating IO into a series of doctrinal documents, *MCDD 3-36 IW / C2W* series, that is intended to overlay IO planning and execution onto the existing Marine Corps planning process.

The Navy, although the controlling department of the Marine Corps, views information warfare integration much differently. The Navy, due to its dispersed battlespace, has long relied on information to conduct both peacetime and wartime operations. The C4I system known as *Copernicus* is at the heart and mind of the entire Navy. Because of these factors, the Navy operates from a significantly more complex and advanced integration program for IW. The Navy has developed several specialized agencies with IW responsibilities ranging from training and doctrine to execution and synchronization.

These specialized agencies plan and execute information warfare at the operational and strategic levels with little affect on the tactical elements.⁶⁰ To the Navy, IW is not a tactical combat multiplier. Information warfare is a series of enabling actions designed to

attain operational or strategic objectives in support of the country's national aims.

According to naval intelligence doctrine, IW/C2W is planned in conjunction with national agencies to achieve information superiority rapidly and if possible defuse any potential crisis. The Navy's entire integration plan is based upon improving intelligence and information flow through existing and developing technology to maintain an operational advantage focused on employment in a crisis situation.

The Air Force's focus is quite similar to the Navy's. The Air Force sees information warfare as a crisis response operation aimed at achieving information superiority through the employment of specialized systems. The Air Force has established specialized squadrons designed to both train in peacetime and execute the AF information campaign in a crisis situation. The Air Force views this specialized squadron much like a JFACC designed for the purpose of achieving superiority through the directed use of all available systems and information.

Much like the Navy, the Air Force operates from a highly centralized system with a rapid response capability that must be structured to address both operational and tactical objectives. Air Force information warfare planning will focus on integrating information capabilities through existing air component commands in support of any established joint warfighting command element.⁶¹ The specialized squadrons, mentioned previously, will assume the lead staff role in planning and controlling the necessary information operations in a theater for the Air Component Commander (ACC). The Air Force is concerned with supporting both joint doctrine and actual warfighting CINCs in the field with their information capabilities.

According to ACOM, this tendency is exactly what the emerging information warfare doctrine is designed to address. Joint doctrine will attempt to capitalize on each services' capabilities while providing a general framework for the planning and execution of information operations in a joint environment. The draft joint doctrine, *JP 3-13, Information Warfare*, is intended to address desired effects, operational and strategic objectives and linkage to national aims. The draft document at present covers tactical employment of elements of IW only in very general terms to allow service and combatant commanders flexibility in application of information systems.⁶²

Achieving these desired effects is the ambiguous portion of the emerging doctrine from the joint and separate service perspectives. Each separate service and ACOM are struggling with whether to approach information warfare/operations from a highly centralized and controlled planning perspective with decentralized execution or a more decentralized comprehensive approach. The real question is actually whether to create a functional command responsible for the joint integration of information warfare or to formulate a strategy which entails each service supporting the combatant commanders in a joint warfighting environment.

Joint Information Operations Alternative

The bottom line is that the majority of future military operations will take place in a joint warfighting environment and therefore, information operations or warfare must also be a focused joint endeavor. JCS must designate some joint agency to take positive control over not only the training and doctrine, but also the execution of information operations on the future battlefield. Detailed inter-service coordination necessary to integrate effective and cohesive information operations is not possible given the current

joint military organizational structure.⁶³ Although ACOM is the emerging proponent responsible for the doctrine and training for joint information operations, there is no single agency responsible for the integrated planning and execution of joint IO. Presently, the Information Warfare Cell under the J3 section of any given CINC staff is responsible for only the planning and execution of C²W.⁶⁴ The responsibility of integration for all services and external agencies for the information operations has not been assigned.

In order to solve this problem, there appears to be two “most probable” courses of action given the existing structure and service capabilities. The first probable course of action for addressing this problem is to create a separate functional command responsible for the doctrine, training, planning, and both peacetime and wartime execution of IO. The second course of action for information operations is simply to limit the scope of IO for the military to address only the C²W aspects and allow the Combatant Commanders to be the military conduits for vertical nesting with the national objectives. This second COA would require close coordination and a delineation of responsibilities between the civilian, government and military participants.

First, when looking at the possibility of creating a separate functional command, two potential scenarios seem most likely. The first scenario would be a short duration task force responsible for information operations given a specific purpose, goal and duration. One possible solution is the creation of a Joint Forces Information Operations Task Force (JFIOTF). The second potential scenario examines a longer term approach to the IO problem with a permanent command element responsible for IO. This solution entails the creation of an Information Operations Command (INFOCOM). There are numerous advantages and drawbacks to each potential solution.

First of all in taking a look at the creation of a JFIOTF, the composition of such a task force would certainly be dependent upon the situation, however, certain considerations would prevail in most circumstances. For example, each JFIOTF would require non-governmental organizations (NGOs), private organizations (PVOs) and governmental agencies, in the form of both military and political, representation for training, planning and execution of the IO. The JFIOTF must be equipped and manned to handle the full range of IO and IW functions with regard to both operational and, if necessary, strategic objectives.

The ultimate objective in establishing a JFIOTF, at the operational level, is to achieve unity of effort and a coordinated application of the existing information instrument of national power to solve any or all potential crises.⁶⁵ The organizational mixture of military, political, NGO and PVO agencies provides the necessary structure to effectively employ information operations at the operational level. The military aspect of IO, C²W, would be a coordinated effort between the Army, Marines Corps, Navy and Air Force services. Although each service would provide IO/IW specialists on this staff, the service who controls the overall military operation would also provide the CINC for the JFIOTF. The NGO, PVO and political representatives would be special advisory staff similar to the organization found in many MOOTW scenarios.

The organizational structure would place the JFIOTF directly under the CINC to enable both operational and strategic information operations. One possible candidate as the JFIOTF commander would be the deputy CINC. This would ensure that there was no service parochialism and also ensure that the strategic interests were addressed. In any event, the JFIOTF would be a supporting command similar to each of the other

component commanders such as the JFLCC or JFACC. The command and control wiring diagram might look something like this:

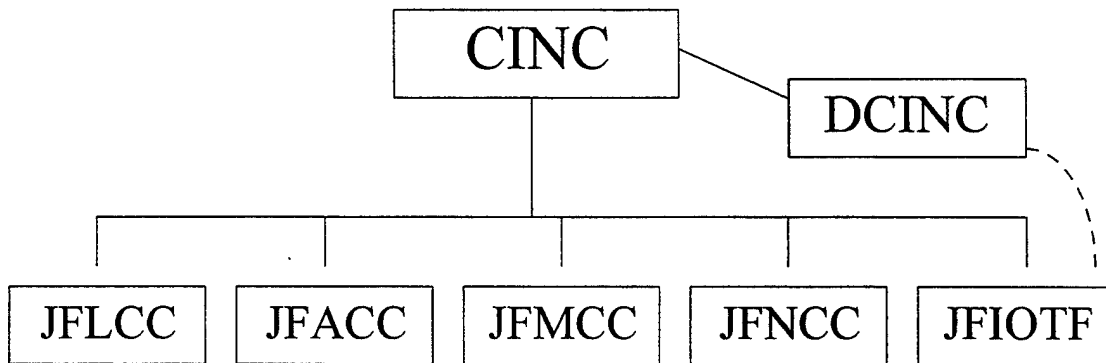


Figure 2. Sample Organizational Chart for JFIOTF Inclusion.

This organization, although limited in duration and scope, would be capable of capitalizing on the synergistic effect of integrating the combined service IO capabilities. The JFIOTF would provide the control but the command element for information operations would remain with the separate services. This organization would be more of a control and tasking organization in order to integrate all aspects of IO without severely disrupting either the existing command or the technical aspects of IO. This task force would enable the operations cell, J3, to focus on the overall execution without requiring additional assets to handle the very complex issue of information operations integration. The other reason for leaving the execution to the separate services is for the simple fact that the expertise and equipment belong to these organizations and it would require far too much lateral movement to bring them together for limited gains.

One of the apparent drawbacks to this temporary task force is that formation of any task force requires time and there would be little time for interagency training and familiarity with C² structure. Another potential drawback is the limited supply of

equipment, communications in particular, and personnel to fill the requirements for such a staff. Given these particular concerns, it is debatable whether this task force is worth the effort for the operational gains obtained through a short term integration of all informational capabilities. Perhaps a more long-term solution to the problem is in order, such as, an existing sub-unified command responsible for global information operations: INFOCOM.

Information Operations Command (INFOCOM) would be a sub-unified command under ACOM responsible for the United States information sovereignty in both peace and wartime. Atlantic Command has already been designated as the joint doctrine proponent and, as the joint force integrator and provider, would be ideally suited to accomplish the integrated joint mission of information operations. Each joint force provided by this sub-unified command would be tailored to the situation's unique requirements or particular mission. This command would include full time coordination cells linked with NGO, PVO and State Department offices in order to provide seamless strategic information operations.

This proposed command structure would enable rapid deployment and support throughout the world in support of any unilateral, joint or even combined operations. The Information Operations Command would also require the technological equipment, manpower and joint staff to plan, coordinate and execute IO throughout any area of responsibility. This full time command structure would enable a cohesive strategy for approaching IO from either a defensive or offensive stance. One of the biggest challenges, however, will be in coordinating with the NGO and PVOs to work toward some common interests.

Operationally, this command could synchronize and exploit the rapid response offensive capabilities of both the Navy and the Air Force in order to establish information superiority or even possibly deter any adversary aggression. INFOCOM would also be able to utilize the stabilizing aspects of either the Army or Marine Corps information operations. Strategically, INFOCOM offers any commander a more effective manner by which he can exploit the information instrument of power while maintaining a definite unity of effort between the services, other governmental and non-governmental agencies.

The creation of such a command as INFOCOM does not alleviate each service's responsibilities with respect to information operations. Each service must continue to develop, train, pursue technological advancements and integration of IO into all operations. INFOCOM is merely the over-arching control mechanism which will provide authoritative guidance, coordinate both offensive and defensive operations and actually de-conflict IO priorities with regard to both the operational and strategic objectives. In short INFOCOM provides the unity of effort and focus for IO that, to date, has not been present. The disjointed service approach to information operations has rapidly advanced forward but with no unity of purpose which leads to the second possible solution.

The second course of action addresses this disjointed approach to IO and how to solve the military problem of focus for IO. This proposal is simply to limit the scope for information operations for the military to address only command and control warfare (C²W). This course of action is more inline with the intended purpose after Desert Storm when General Colin Powell attributed the U.S. success to "information age warriors."⁶⁶ The military was not looking for information managers, but warriors that were capable of exploiting information and information technologies.

By limiting the scope of IO for the military to only the C²W aspects, a much more focused approach toward inter-service and interagency integration can be accomplished. This COA does not call for an organizational change or shift in present focus. Focusing in on the C²W aspects merely allows the services to handle the military aspects in support of other governmental agencies addressing the strategic and political aspects of IO. The doctrine and training responsibilities can remain with ACOM but the execution responsibilities for IO would reside with the CINCs operationally and the NCA at the national strategic level.

With this proposed structure, the military C²W focus would be more at the operational and tactical levels. This is in line with what the services presently see as their role and responsibility for information operations or warfare. Each separate service acknowledges that, if called upon, it may have to operate in support of national strategic aims, but it is agreed that this is not their primary focus. The Joint Chiefs of Staff first started out to integrate the services information operations capabilities with regard to C²W. As mentioned previously, this has remained the common ground for each service with respect to information operations or warfare. Both joint and service component doctrine exists for command and control warfare and the only part left to transform would then be the integrated execution of C²W.

The agency responsible for the integrated execution of C²W must be a joint agency with connectivity to non-governmental and governmental agencies similar to the previously mentioned INFOCOM. One possible solution would be to have a combatant command function as both the command and control agency for C²W and also serve as the conduit for vertical nesting with the desired national objectives. This COA, unlike the

JTF proposal, would required an extremely strong agreement and operational relationship with both civilian and other governmental agencies. This would be necessary to ensure a clear delineation of responsibilities and execution strategies.

This course of action has one definite drawback in that it still does not fix the problem of operational integration for either C²W or IO in execution. Simply stating that it is a CINC's responsibility without resourcing these headquarters is not the answer. In order for the military to solve the existing problem, the changes must entail more than just a shift in focus and they must also consider the resource and monetary limitations placed on the military today. Simply focusing on the C²W aspects of IO is exactly what the services want because they are prepared to handle this mission, but it is not in the best joint interests for the entire military.

The military can not afford this narrow-minded approach given the probability of operating in both conventional and unconventional environments on future battlefields. In order to achieve informational, or any other, unity of effort, requires coordination and realignment of organizational thought and operation to achieve information superiority within any given environment the military is called upon to operate.⁶⁷

Conclusion

The result of what is written in this paper does not dispute the importance nor the relevance of information operations or warfare. On the contrary, information has and probably will continue to be one of the most vital national and military instruments of power. This paper does, however, focus on answering the question of what approach should the Department of Defense (DOD) take to fully incorporate information warfare or operations on the future battlefield. The answer, although complex in analysis, is simply

that DOD should create a sub-unified command, Information Operations Command (INFOCOM), under USACOM responsible for the country's information sovereignty in both peace and wartime.

George J. Stein captured this conceptual shift best when he stated that "adopting information technologies as force multipliers without changing the way business is done may be the greatest single threat faced by the services."⁶⁸ In comparing the proposed organizational revisions, there are several reasons why this suggested organizational change is more beneficial to information operations on the future battlefields. The first reason is that to be successful every military operation must have a clearly defined command and control structure both in peace and wartime. The military is extremely flexible but the existing structure is what allows the military to operate in this manner.

This C² structure, on today's and future battlefields, must also integrate non-governmental and political agencies to ensure linkage to the national strategic objectives. At present there is no existing operational command and control structure to accomplish this task. The creation of Information Operations Command would provide this necessary C² structure from which all operations could emanate.

The second reason is that at present there are no combined effects gained from the employment of information operations. Each separate service has its own agreed upon definitions, purpose and methods of employment. The joint doctrine put forth in manuals such as *JP 3-13.1, Command and Control Warfare*, *JP 1-02, DOD Dictionary of Terms* and *MOP Number 30, Command and Control Warfare (C²W)* are not authoritative in nature and adhered to as doctrine by the services. With an ever decreasing military force structure, safeguarding and promoting our nation's interests will required an

unprecedented unity of effort between not only all of the services but also every instrument of national power.⁶⁹

The third reason is that an existing command and control structure will enable the military to fully incorporate the rapid response capabilities of such services as the Navy and combine these with the perseverance of a land component such as the Army. No short term organization could accomplish this diverse mission while maintaining both horizontal and vertical connectivity. The JFIOTF could accomplish this mission but only after an initially longer period of time to establish the task force and the growing pains associated with any new organization.

As mentioned previously, the establishment of such an organization as INFOCOM is not without significant cost and potential discomfort from realigning headquarters and existing C² structures. The question then becomes whether the operational military gains will outweigh the initial entry cost or whether the U.S. military force can afford not to accept such an organizational paradigm shift given the evolving nature of warfare. This is the baseline question to be answered as the military moves forward into the future.

Information and information technology is indeed one of the most sought after resources both today and into the foreseeable future. The resource itself is critical but no more critical than the means to control and effectively employ it. The existence of a command such as INFOCOM is one of the means by which the military can effectively accomplish the NMS and gain information superiority. If the ultimate goal of both information operations and warfare is truly the achievement of information superiority, then the military can ill afford to not establish a structure that is capable of both command and control of both information operations and information warfare.

ENDNOTES

1. Carl von Clausewitz, On War translated by Michael Howard and Peter Paret, (Princeton, New Jersey). P. 75.
2. Alvin Toffler, The Third Wave, (New York: Bantam Books, 1980), p. 6. This idea is a synopsis of his ideas on transitioning from an industrial age into the information age with respect to the military.
3. Rick Brennan and R. Evan Ellis, *Information Warfare in Multilateral Peace Operations – A Case Study of Somalia*, Report to the Secretary of Defense, (Washington, D.C.: SAIC, 1996), p. 38.
4. United States, Department of the Army, TRADOC Pamphlet 525-5: Force XXI Operations, (Fort Monroe, VA: Army Training and Doctrine Command, 1 August 1994), p. 1-5.
5. Morris, William, American Heritage Dictionary, (Boston, Houghton Mifflin Co., 1995), p.675.
6. United States, Department of the Army, Field Manual 100-6: Information Operations, (Washington, D.C.: GPO, 6 December 1995), p. 2-1.
7. JCS Publication 1-02, DOD Dictionary of Definitions and Terminology, JEL, March 1997.
8. George J. Stein, *Information Warfare*, (available from <http://www.cdsar.af.mil/apj/szfran.html>, Internet, accessed 12 December 1997), p.3.
9. United States, Department of the Army, Field Manual 100-5: Operations, (Washington, D.C.: GPO, June 1993), p. Glossary-9.
10. Martin van Crevald, The Transformation of War, (New York: Free Press, 1991), pp196-203. This is a synopsis of van Crevald's explanation of the significant differences between war and warfare. His central point is that Clausewitzian war as we know it is probably a thing of the past but warfare is not.
11. Office of the Secretary of Defense, Defense Science Board Task Force on Information Warfare - Defense (IW-D), (DSB Report), (Washington, D.C.: GPO, 1996), Enclosure p.5.
12. Field Manual 100-6: Information Operations, p. 2-3.
13. Ibid., p. 2-3.
14. Ibid., p. 1-9.
15. Ibid., p. 3-2.

ENDNOTES

16. Field Manual 101-5-1: Operational Terms and Graphics, (Washington, D.C.: GPO, 1998), Glossary.
17. Robert Thompson, *Information Warfare: Part 2*, Kaman Science Corp., (URL www.dacs.com/awareness/newsletters/summer96/dod.structure.html, accessed 12 February 1998), p.4.
18. Field Manual 100-6: Information Operations, p. 2-1.
19. Naval Intelligence, *Joint Electronic Library (JEL)*,
20. Admiral J. M. Boorda, *Copernicus Forward: C4I for the 21st Century*, (URL www.navy.mil/copernicus., accessed 21 January 1998), p. 1.
21. Ibid., p. 2.
22. Naval Intelligence Publication, *Joint Electronic Library (JEL)*,
23. *Copernicus Forward: C4I for the 21st Century*, p.6.
24. *Information Warfare: Part 2*, Kaman Science Corp., p.2.
25. Thomas Eipp, Information Operations: A Marine Corps Concept Paper (MCCP), (U.S. Marine Corps Doctrine Division, Quantico, Va., November 1997), accessed at <http://138.156.107.3/concepts/IO.htm>, p.3. This is a concept paper that according to LTC Baisol of the Marine Corps Doctrine Division is shaping the thinking in the production of the new Marine Corps Doctrinal Publication (MCDP 36-2) on Information Operations.
26. Ibid., p.2.
27. Ibid.
28. COL G.I. Wilson and MAJ Frank Bunkers, *Uncorking the Information Genie*. Marine Corps Gazette, October 1995, accessed on 21 December 1998 at URL www.eajardines.com/marine.html, p.5.
29. Information Operations: A Marine Corps Concept Paper (MCCP), p. 8.
30. United States, Department of the Air Force, Air Force Doctrinal Document 2-5, Maxwell AFB, Alabama, December 1997, p. 5.
31. Ibid., p. 4.
32. Ibid., p. 7.
33. *Information Warfare: Part 2*, Kaman Science Corp., p. 3.

ENDNOTES

34. Sheila E. Widnall, Cornerstones of Information Warfare, Accessed on 17 December 1997 from <http://www.af.mil/lib/corner.html>, p. 3. This paper is a compilation of the Secretary of the Air Force Ms. Widnall's and the Air Force Chief of Staff, General Fogelman's thoughts and guidance on a comprehensive approach to information operations.
35. *Ibid.*, p. 5.
36. Air Force Doctrinal Document 2-5, p.7.
37. *Information Warfare*, (available from <http://www.cdsar.af.mil/apj/szfran.html>, Internet, accessed 12 December 1997), p.10.
38. Office of the Joint Chiefs of Staff, Joint Publication 1-02: DOD Dictionary of Terms, (Washington, D.C.: GPO, JEL, May 1997), p. 263.
39. Office of the Joint Chiefs of Staff, Joint Vision 2010, (Washington, D.C.: GPO, JEL, May 1997), p.42.
40. *Ibid.*, p.41.
41. *Ibid.*
42. United States, Department of Defense, DOD Directive S-3600.1 Information Operations, (Washington, D.C.: 9 December 1996), p.6.
43. *Ibid.*, p.12.
44. Phone interview with LCMR Paul Stevenson, Atlantic Command Information Warfare PO. This phone conversation was conducted on 27 January 1998 and was concerning the unclassified material and status of the new doctrinal manual *JP 3-13 Information Warfare*. The status of the manual is actually behind schedule due to the extensive comments from the joint field on the subject matter.
45. Joint Vision 2010, p. 52.
46. DOD Directive S-3600.1 Information Operations, p. 9.
47. Joint Vision 2010, p. 50.
48. Phone interview with LCMR Paul Stevenson, Atlantic Command Information Warfare PO. This comment was provided by LCMR Stevenson as to the focus for the emerging doctrine provided in the CINC's guidance to his staff concerning IW/IO.

ENDNOTES

49. Ibid. Conversation was an attempt to find out how ACOM envisions the future of information warfare developing. ACOM is not sure what approach will provide the answers and has initially proposed that possible scenarios be tested in a Battle Lab environment.
50. This comment is a summary of a central theme in both the Army's FM 100-6: Information Operations, and the Marines Information Operations: A Marine Corps Concept Paper (MCCP). Both services feel that they are not deterrent forces in the medium of information operations. They both feel that their role is more one of stabilizing an existing crisis or supporting larger scale information operations from the strategic level.
51. Ibid.
52. Daniel E. Magsig, "Information Warfare: In the Information Age," Available from <http://www.magsig@comm.hq.af.mil>; accessed on 16 December 1997, p. 7.
53. Phone Interview with LTC Carl Walker, Marine Corps Doctrinal Division, Quantico, Va. on 8 December 1997 concerning the Marine Corps emerging doctrine for Information Operations. His conversation was focused on the fact that the Marine Corps had read the Army publications and was producing something very similar to the Army's approach to IO. At present the Marine Corps has three information operations manuals in progress.
54. Ibid. LTC Walker's comments indicated that Marine Corps doctrine has always been an attempt to address tactical and operational level doctrine from both a land and sea perspective. Information operations, however, is one doctrinal concept that the Marines are taking more a land-based approach and allowing the Navy to dictate the sea-borne doctrine as to its employment.
55. Martin C. Libicki, What is Information Warfare?, (Washington, D.C.: National Defense University, 1995), p. 36.
56. United States, Department of the Air Force, Air Force Doctrinal Document 2-5, p. 5.
57. Ibid.
58. J. Ryan, Information Support to Military Operations in the Year 2000 and Beyond: Security Implications, Center for Naval Analysis, Alexandria, Virginia, 1993, p. 17.
59. Office of the Joint Chiefs of Staff, Command and Control Warfare (C²W), Memorandum of Policy No. 30, (Washington, D.C.: 8 March 1993), p.24.
60. George F. Kraus, "Information Warfare in 2015," *U.S. Naval Institute Proceedings*. 121 (August 1995), p.43.
61. United States, Department of the Air Force, Air Force Doctrinal Document 2-5, p. 7.

ENDNOTES

62. Phone interview with LCMDR Paul Stevenson, Atlantic Command Information Warfare PO. The entire paragraph is a summary of the phone conversation's unclassified references to the projected aims of the draft joint doctrinal manual, *JP 3-13 Information Warfare*. These views may change but at present they are the most up to date references to joint information warfare doctrine.
63. Matt. Straughan, Information Operations and Unity of Effort: The Case for a Joint Interagency Information Operations Task Force, (U.S. Naval War College, Newport, Rhode Island, 1997), p.3.
64. Office of the Joint Chiefs of Staff, Joint Publication 3-13.1: Joint Doctrine for Command and Control Warfare (C²W), (Washington, D.C.: GPO, JEL, 7 February 1997), p. 4.
65. Matt Straughan, Information Operations and Unity of Effort: The Case for a Joint Interagency Information Operations Task Force, (U.S. Naval War College, Newport, Rhode Island, 1997), abstract. Concept was taken from the abstract of this paper, however, it is expanded upon during the first two sections of the paper.
66. Gregory G. Barac, Interoperability: The Cornerstone of Information Warfare, (U.S. Army War College, Carlisle Barracks, Pennsylvania, 1996), p. 2.
67. Office of the Joint Chiefs of Staff. Joint Publication 0-2: Unified Action Armed Forces (UNAAF). (Washington, D.C.: GPO, JEL, February 1995), p. 1-3.
68. George J. Stein, *Information Warfare*, p. 32.
69. Matt Straughan, Information Operations and Unity of Effort: The Case for a Joint Interagency Information Operations Task Force, p. 1.

Bibliography

Books

- Bellamy, Christopher. The Evolution of Modern Warfare: Theory and Practice. New York: Routledge, 1990.
- Beniger, James R. The Control Revolution: Technological and Economic Origins of the Information Society. Cambridge: Harvard University Press, 1986.
- Griffith, Samuel B., ed., Sun Tzu: Art of War. London: Oxford University Press, 1971.
- Hunnington, Samuel P. The Clash of Civilizations and the Remaking of the World Order. New York: Simon Schuster, 1996.
- Johnson, Stuart E. and Martin C. Libicki. Dominant Battlespace Knowledge. Washington, D.C.: National Defense University, 1996.
- Kelly, Kevin. Out of Control. Reading, MA: Addison-Wesley, 1994.
- Libicki, Martin C. What is Information Warfare?. Washington, D.C.: National Defense University, 1995.
- Libicki, Martin C. The Mesh and the Net. Washington, D.C.: National Defense University, August 1995.
- Morris, William. American Heritage Dictionary. Boston, Houghton Mifflin Co., 1995.
- Nichiporuk, Brian and Carl H. Builder. Information Technologies and the Future of Land Warfare. Rand Arroyo Center, Santa Monica, CA, 1995.
- Schwartau, Winn. Information Warfare. New York: Thunder's Mouth Press, 1994.
- Toffler, Alvin. The Third Wave. New York: Bantam Books, 1980.
- Toffler, Alvin and Heidi. War and Anti-War: Survival at the Dawn of the 21st Century. Boston: Little, Brown and Company, 1993.
- Van Crevald, Martin. The Transformation of War. New York: Free Press, 1991.
- Von Clausewitz, Carl. On War. Edited and translated by Michael Howard and Peter Paret. Princeton: Princeton University Press, 1976.
- Waldrop, M. Mitchell. Complexity: The Emerging Science at the Edge of Order and Chaos. New York: Simon and Schuster, 1992.

Military Publications

Office of the Joint Chiefs of Staff. Command and Control Warfare (C²W). Memorandum of Policy No. 30. Washington: 8 March 1993.

Office of the Joint Chiefs of Staff. Joint Vision 2010. Washington, D.C.: GPO, JEL, May 1997.

Office of the Joint Chiefs of Staff. Joint Publication 0-2: Unified Action Armed Forces (UNAAF). Washington, D.C.: GPO, JEL, February 1995.

Office of the Joint Chiefs of Staff. Joint Publication 1-02: DOD Dictionary of Terms. Washington, D.C.: GPO, JEL, May 1997.

Office of the Joint Chiefs of Staff. Joint Publication 3-0: Joint Operations. Washington, D.C.: GPO, JEL, May 1997.

Office of the Joint Chiefs of Staff. Joint Publication 3-13.1: Joint Doctrine for Command and Control Warfare (C²W). Washington, D.C.: GPO, JEL, 7 February 1997.

Office of the President of the United States. Executive Order # 12864: United States Advisory Council on the National Information Infrastructure. Washington, D.C.: GPO, September 1993. Available from the Internet <http://library.whitehouse.gov>; accessed 21 Dec 97.

Office of the Secretary of Defense. Defense Science Board Task Force on Information Warfare - Defense (IW-D). (DSB Report), Washington, D.C.: GPO, 1996.

United States, Department of the Air Force. Air Force Doctrine Document 1. Maxwell AFB, Alabama, September 1997.

United States, Department of the Air Force. Air Force Doctrinal Document 2-5. Maxwell AFB, Alabama, December 1997.

United States, Department of the Army. Field Manual 100-6: Information Operations. Washington, D.C.: GPO, 6 December 1995.

United States, Department of the Army. Field Manual 100-5: Operations. Washington, D.C.: GPO, 1993.

United States, Department of the Army. Field Manual 101-5: Staff Organizations and Operations. Washington, D.C.: GPO, 1997.

United States, Department of the Army. Field Manual 101-5-1: Operational Terms and Graphics. Washington, D.C.: GPO, 1998.

United States, Department of the Army. TRADOC Pamphlet 525-5: Force XXI Operations. Fort Monroe, VA: Army Training and Doctrine Command, 1 August 1994.

United States, Department of Defense. DOD Directive S-3600.1 Information Operations. Washington, D.C.: GPO, 9 December 1996.

United States, Department of Defense. Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance. Washington, D.C.: DOD, 1996.

United States, Department of the Navy. FMFM-1 Warfighting. Washington, D.C.: GPO, 6 March 1989.

United States, National Defense University. Strategic Assessment 1997: Instruments of U.S. Power. Washington: Institute for National Strategic Studies, National Defense University, 1997.

Papers

Barac, Gregory G. Interoperability: The Cornerstone of Information Warfare. U.S. Army War College, Carlisle Barracks, Pennsylvania, 1996.

Barlow, W.J. Information Warfare: Selected Long-Range Technology Applications (IDA Paper P-3157). Washington, D.C.: Institute for Defense Analysis, February 1996.

Blasche, Theodore R. and Lickteig, Carl W. Utilization of a Vehicle Integrated Intelligence System in Armor Units. Research Project, U.S. Army Institute of the Behavioral and Social Sciences, Fort Knox, Kentucky: 1984.

Brennan, Rick and Ellis, R. Evan. *Information Warfare in Multilateral Peace Operations – A Case Study of Somalia*. Report to the Secretary of Defense. Washington, D.C.: SAIC, 1996.

Buchan, Glenn. Information Warfare and the Air Force: Wave of the Future? Current Fad? URL www.rand.org/publications/IP/IP149, 1997.

Doyle, Kevin J. Information Operations: A Look at Emerging Doctrine and its Operational Implications. School of Advanced Military Studies Monograph, U.S. Army Command and General Staff College, Fort Leavenworth, Kansas, 1995.

Eipp, Thomas. Information Operations: A Marine Corps Concept Paper (MCCP). U.S. Marine Corps Doctrine Division, Quantico, Va., November 1997, accessed at <http://138.156.107.3/concepts/IO.htm>.

Jordan, M.E. Command and Control Warfare. U.S. Air Force War College, Maxwell Air Force Base, Alabama, March 1985.

- Kohlman, James P. Winning the Information War: Challenges of Providing Interoperable Information System Support to an Army-Led Joint Task Force. U.S. Army Command and General Staff College, Fort Leavenworth, Kansas, 1994.
- McLendon, J. Information Warfare: Impact and Concerns. U.S. Air Force War College, Maxwell Air Force Base, Alabama, 1994.
- Paylor, M. Command and Control in Future Warfare. U.S. Naval War College, Newport, Rhode Island, 1996.
- Plucker, R.C. Command and Control Warfare - A New Concept for the Joint Operational Commander. U.S. Naval War College, Newport, Rhode Island, 1993.
- Ryan, J. Information Support to Military Operations in the Year 2000 and Beyond: Security Implications. Center for Naval Analysis, Alexandria, Virginia, 1993.
- Schneider, James J. "Black Lights: Chaos, Complexity and the Promise of Information Warfare." School of Advanced Military Studies, Fort Leavenworth, Kansas, 1996.
- Stewart, M. Information Operations, Information Warfare: Policy, Perspective and Potential Problems. U.S. Army War College, Carlisle Barracks, Pennsylvania, 1997.
- Straughan, Matt. Information Operations and Unity of Effort: The Case for a Joint Interagency Information Operations Task Force. U.S. Naval War College, Newport, Rhode Island, 1997.
- Widnall, Sheila E. Cornerstones of Information Warfare. Accessed on 17 December 1997 from <http://www.af.mil/lib/corner.html>.

Articles

- Boorda, Admiral J. M.. *Copernicus Forward: C4I for the 21st Century*. URL www.navy.mil/copernicus., accessed 21 January 1998.
- DeCaro, Chuck. "Softwar". AFCAE Anthology of Information Warfare, April 1996.
- Dinardo, R.L. and Daniel J. Hughes. "Some Cautionary Thoughts on Information Warfare." *Airpower Journal*. (December 1995): 69.
- Dupont, Daniel G. and Richard Lardner. "Force XXI: The Long and Windy Road to the Army of the Future." *Armed Forces Journal*. (October 1994): 45-51.
- Iselin, Errol. "The Impact of Information Diversity on Information Overload Effects in Unstructured Managerial Decision Making," *Journal of Information Science*. 15 (July 1989): 163-173.

Fogelman, Ronald R. *Cornerstones of Information Warfare*. URL www.af.mil/lib/corner.html, 1996.

Hammes, Thomas X. "The Evolution of War: The Fourth Generation." *Marine Corps Gazette*. 78, no. 9, September 1994.

Kuehl, Daniel T. "Strategic Information Warfare and Comprehensive Situational Awareness". Washington, D.C.: Department of Defense White Paper, 1996.

Kraus, George F. "Information Warfare in 2015." *U.S. Naval Institute Proceedings*. 121 (August 1995): 42-45.

Magsig, Daniel E. "Information Warfare: In the Information Age." Available from <http://www.magsig@comm.hq.af.mil>; accessed on 16 December 1997.

Mann, Edward. "Desert Storm: The First Information War?" *Airpower Journal*, Volume 8, (Winter 1994): 4-13.

Nye, Joseph, William Owens, and Eliot Cohen. *The Information Edge*, Foreign Affairs. Volume 75, No. 2, March/April 1996.

Peters, Ralph. "After the Revolution." *Parameters*. Vol. XXV, No. 5 (Summer 1995), pp. 7-14.

Stein, George J. *Information Warfare*. Available from <http://www.cdsar.af.mil/apj/szfran.html>; internet; accessed 12 December 1997.

Sullivan, Gordon R. and James M. Dubik. *Envisioning Future Warfare*. Fort Leavenworth, KS: US Army Command and General Staff College Press, 1995, pp. 43-62.

Szafranski, COL Richard. *A Theory of Information Warfare: Preparing for 2020*. Airpower Journal, Volume 9, No. 1, Spring 1995.

Wilson, COL G.I. and MAJ Frank Bunkers. *Uncorking the Information Genie*. Marine Corps Gazette, October 1995, accessed on 21 December 1998 at URL www.eajardines.com/marine.html.

Other References

Stevenson, LCDMR Paul. Phone interview conducted on 27 January 1998. LCDMR Stevenson is one of the Atlantic Command Information Warfare Project Officers. The unclassified comments for the IW manual will be available on the ACOM Homepage sometime in 1999.

Walker, LTC Carl. Phone interview conducted on 8 December 1997. LTC Walker works at the Marine Corps Doctrinal Division in Quantico, Virginia. This conversation was focused on determining the Marine Corps stance on Information Warfare or Operations. This discussion also involved determining the influence of the Army and Navy on Marine Corps doctrine development.